



# UNITED STATES PATENT AND TRADEMARK OFFICE

ET

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/036,521

01/07/2002

Robert John Ackroyd

01.119.01

5107

7590

07/26/2006

Zilka-Kotab, PC  
P.O. Box 721120  
San Jose, CA 95172-1120

EXAMINER

SHIFERAW, ELENI A

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 07/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/036,521

Applicant(s)

ACKROYD, ROBERT JOHN

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 17 May 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## **DETAILED ACTION**

### ***Response to Amendment***

1. Applicant's arguments with respect to claims 1-27 have been fully considered but are not persuasive. And also arguments are moot in view of the new ground(s) of rejection.

### ***Response to Arguments***

2. Argument is not persuasive. Applicant's argument regarding limitations "detecting code for detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger...", Schertz et al. discloses networkbased intrusion protection system and/or inline intrusion protection system, and/or Schertz et al. teaches virus intrusion detecting/monitoring/scanning of **ALL devices on a network network-wide**, network-based virus intrusion detection system typically monitors all network activity and network traffic, Network-based virus intrusion protection systems analyze data inbound from the internet and collects network packets to compare against a database of various known attack signatures or bit patterns (see (par. 21, 23, and par. 0018).

And also Hypponen et al. teaches a virus scanning server 7 scanning and detecting the received suspicious log data using F-PROT TM, and F-SECURE

TM, and/or detecting virus on a network-wide connected computer.

Detected/suspected data packets coming in from outside world, from network 5, connected computers or coming out from Internet 1 are compared with known virus signature (par. 0036, 0035, and fig. 1).

Regarding claim 6, argument is not persuasive. Firstly, the Applicant has never argued before when applicant files an argument and/or amendment for more than two times in his responses. Secondly, Schertz discloses **preventing a transmission of payload to other hosts and discarding data identified as being associated with an attack** when malware is detected and anti-malware action performed that is isolating the transmitter computer from host or other computers (see par. 0031 lines 17-26, and 0020 lines 14-17).

Regarding claim 7, argument is not persuasive. Firstly, the Applicant has never argued before when applicant files an argument and/or amendment for more than two times in his responses. Secondly, Schertz discloses Network Intrusion Protection Devices 80 and 81 contains known attack signatures log data messages with the databases 80a and 81a (see, fig. 2 No. 80A and 81A and par. 0021 lines 15-18).

Regarding claim 4, Argument is not persuasive. Firstly, applicant has never argued regarding claim 4 until filing RCE. Secondly, Schnurer discloses the well-known pattern/signature updates by updating the antivirus software (Schnurer col. 5 lines 16-19). The Examiner further provides another reference for the applicant's reference to show this argument is well known. Butt et al.

US PG PUBS 2003/0055963A1 and Presotto et al. US PG PUBS 20030110395 disclose updating the antivirus software to update patterns, because it would include the newer pattern signatures.

With regards to claim 5, Argument is not persuasive. Firstly, applicant has never argued regarding claim 4 until filing RCE. Secondly, Chen discloses performing more thorough virus scanning after virus is detected (see, Fig. 3 No. 260). Sufficient motivation to combine the applied references is provided in the office action mailed on 02/21/2006. Accordingly all claims are stand rejected.

***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-3, 6-12, 15-21, and 24-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Schertz et al. (Schertz, Pub. No.: US 2003/0084322 A1).

As per claims 1, 10, and 19, Schertz teaches a computer program product/method/apparatus for controlling a managing computer to manage malware protection within a computer network containing a plurality of network connected computers, said computer program product comprising:

receiving code operable to receive at said managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers (page 4 par. 0030 lines 9-10, and page 3 par. 0022 lines 8-10);

detecting code operable to detect from said plurality of log data messages received by said managing computer a pattern and **a network-wide threshold (par. 21, 23, and par. 0018 of Schertz discloses: *virus intrusion***

***detecting/monitoring/scanning of ALL devices on a network network-wide, network-based virus intrusion detection system typically monitors all network activity and network traffic, Network-based virus intrusion protection systems analyze data inbound from the internet and collects network packets to compare against a database of various known attack signatures or bit patterns)*** of malware detection across said plurality of network connected computers matching one or more predetermined trigger, (page 4 par. 0030 lines 9-21, page 3 par. 0021 lines 10-18, and par. 0023 lines 12-18) ***the network-wide threshold being applied to a sum of detections each being associated with a different one of the network connected computers (0003, 0018; a network based system monitoring all network***

***activity and network traffic by collecting packets that has patterns transmitted from multiple network user computers and compare patterns against a database of various known attack signatures*** ); and

action performing code operable in response to detection of one or more predetermined trigger patterns to perform one or more predetermined anti-malware actions (page 4 par. 0030 lines 16-21, and page 3 par. 0020 lines 14-25).

As per claims 2, 11, and 20, Schertz teaches a computer program product/method/apparatus, wherein said plurality of network connected computers each have a malware scanner that serves to scan computer files to detected malware within said computer files (page 4 par. 0031 lines 1-3).

As per claims 3, 12, and 21, Schertz teaches a computer program product/method/apparatus, wherein said malware scanner uses malware definition data to identify malware to be detected (page 4 par. 0031 lines 1-3, and fig. 1 No. 16).

As per claims 6, 15, and 24, Schertz teaches a computer program product/method/apparatus, wherein said one or more predetermined anti-malware actions include isolating one of more of said network connected computers from other parts of said computer network (page 4 par. 0031 lines

17-24 and page 3 par. 0020 lines 14-17).

As per claims 7, 16, and 25, Schertz teaches a computer program product/method/apparatus, wherein said managing computer stores said plurality of log data messages within a database (fig. 2 No. 80A and 81A).

As per claims 8, 17, and 26, Schertz teaches a computer program product/method/apparatus, wherein said detecting code is operable to query said database (page 18 lines 7-10).

As per claims 9, 18, and 27, Schertz teaches a computer program product/method/apparatus, wherein said database includes data identifying one or more of:

- malware protection mechanisms used by respective network connected computers (page 2 par. 0016 lines 14-17);

- versions of malware protection computer programs used by respective network connected computers (page 4 par. 0031 lines 1-3, and fig. 1.No. 16);

- versions of malware definition data used by respective network connected computers (page 4 par. 0031 lines 1-3, and fig. 1 No. 16); and

- security settings of malware protection mechanisms used by respective network connected computers (page 2 par. 0016 lines 14-17).



As per claim 28, Schertz discloses a program stored on a computer-readable medium as claimed in claim 1, wherein predefined network-wide thresholds and patterns are provided as templates (0021 lines 15-18; *network-wide patterns are provided as a template*).

As per claim 29, Schertz discloses a program stored on a computer-readable medium as claimed in claim 1, wherein predefined network-wide thresholds and patterns are customized to particular circumstances (0021; *customized to ... detecting, comparing circumstances...*)

### ***Claim Rejections - 35 USC § 103***

5. Claims 4, 13, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schertz et al. (Schertz, Pub. No.: US 2003/0084322 A1) in view of Schnurer et al. (Schnurer, Patent Number: 5842002).

As per claims 4, 13, and 22, Schertz teaches all the subject matter as described above.

Schertz do not explicitly teach updating of malware definition data.

However Schnurer teaches a computer program product/method/apparatus, wherein said one or more predetermined anti-malware actions include forcing

an update of malware definition data being used by one or more of said plurality of network connected computers (Schnurer col. 5 lines 16-19).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Schnurer within the system of Schertz because it would keep the detection device current (Schnurer col. 5 lines 16-19).

6. Claims 5, 14, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schertz et al. (Schertz, Pub. No.: US 2003/0084322 A1) in view of Chen et al. (Chen, Patent Number: 5,832,208).

As per claims 5, 14, and 23, Schertz teaches all the subject matter as described above.

Schertz does not explicitly teach altering the scanner setting when malware is detected.

However Chen teaches a computer program product/method/apparatus, wherein said one or more predetermined anti-malware actions include altering at least one scanner setting of at least one malware scanner such that said malware scanner performs more thorough malware scanning (Chen Fig. 3 No. 260; performing more thorough virus scanning after virus is detected).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Chen within the system of Schertz because it would scan the entire email/data to detect more virus if any.

7. *Claims 1, 10, and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Chefalas et al. US PG PUBS 2002/0116639 A1.*

*As per claims 1, 10, and 19, Schertz teaches a computer program product/method/apparatus for controlling a managing computer to manage malware protection within a computer network containing a plurality of network connected computers (fig. 1 and claim 29), said computer program product comprising:*

*receiving code operable to receive at said managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers (0057-0058; identified malware detections are received at the server 106 from plurality of client devices over the networks);*

*detecting code operable to detect from said plurality of log data messages received (0012, fig. 4A-B, fig. 5A-B are detected at users computers and received at the server) by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching one or more predetermined trigger (0012, fig. 4A-B, fig. 5A-B; multiple patterns are detected and transmitted to the server network-wide threshold), the network-wide threshold being applied to a sum of detections each being associated with a different one of the network connected computers (0012, 0022-0024 and 0057-0058; multiple different/sum of detections network-wide is performed in multiple client computer stations); and*

*action performing code operable in response to detection of one or more predetermined trigger patterns to perform one or more predetermined anti-malware actions (0012 and fig. 8 element 804).*

8. Claims 1, 10, and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Hypponen et al. US 2003/0191957 A1.

As per claims 1, 10, and 19, Hypponen et al. teaches a computer program product/method/apparatus for controlling a managing computer to manage malware protection within a computer network containing a plurality of network connected computers (fig. 1 and 2), said computer program product comprising:

receiving code operable to receive at said managing computer (*virus scanning server 7*) a plurality of log data messages identifying detection of malware (*detecting and identifying suspicious virus contained data packets and suspicious virus log data received by server 7*) by respective ones of said plurality of network connected computers (par. 0036, 0035, and fig. 1; *detecting virus on a network-wide connected computers... detected/suspected data packets coming in from outside world (from network 5) connected computers or coming out (from internet 1) are compared with known virus signature*);

detecting code operable to detect from said plurality of log data messages received by said managing computer a pattern (par. 0036; *virus scanning server 7 scanning and detecting the received suspicious log data using F-PROT TM, and*

*F-SECURE TM*) and a **network-wide threshold** of malware detection across said plurality of network connected computers matching one or more predetermined trigger, ***the network-wide threshold being applied to a sum of detections each being associated with a different one of the network connected computers*** (par. 0036, 0035, and fig. 1; *detecting virus on a network-wide connected computers... detected/suspected data packets coming in from outside world multiple network client computers, from network 5, connected computers or coming out from internet 1 are compared with known virus signatures*); and

action performing code operable in response to detection of one or more predetermined trigger patterns to perform one or more predetermined anti-malware actions (par. 0037 lines 6-8, 0038, and fig. 2; *in the event that a virus is identified by the virus scanning server 7, the server may take one of a number of different courses of ACTION i.e. disinfecting/removing, quarantine/isolating, notifying...*).

### **Conclusion**

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 2004/0230840 A1 Radatti: discloses *viruses, Trojan, horses, worms, and etc... detection over a network. Receiving and detecting all data streams that pass from an external network, through the*

*transport layer of an operating system to the user application or fro the user application to the transport layer.*

US 2004/0088570 A1 Roberts et al. *discloses internet data malware scanning.*

US 2003/0177397 A1 Samman *discloses network environment virus detection and protection.*

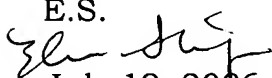
US 2003/0023866 A1 Hinchliffe et al. *discloses centrally managed malware scanning and detecting method.*

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

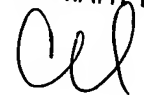
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.

  
July 19, 2006

CHRISTOPHER REVAL  
PRIMARY EXAMINER

 7/24/06